PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-218851

(43)Date of publication of application : 31.07.2003

(51)Int.Cl. H04L 9/08
G06F 12/00
G06F 12/14
G09C 1/00

(21)Application number : 2002-359963

(22)Date of filing : 11.12.2002

(71)Applicant : PERVASIVE SECURITY SYSTEMS INC

(72)Inventor : GARCIA DENIS JACQUES PAUL

(30)Priority

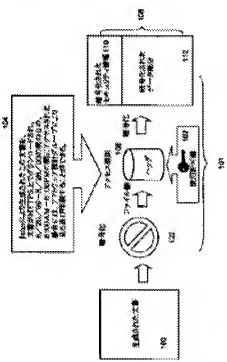
Priority number	Priority date	Priority country
2001 339634	12.12.2001	US
2002 074804	12.02.2002	US
2002 159537	31.05.2002	US

(54) METHOD AND APPARATUS FOR SAFEGUARDING DIGITAL ASSET

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a further effective method for continuously safeguarding and at the same time protecting a digital asset.

SOLUTION: When a safeguarded file is secret even if a proper access right is given, at least a security use permission key is required. The secured file has two portions, namely a header portion and a secured data portion. The header includes security information that indicates or includes an access rule, a protection key, and a file key. The access rule facilitates access to the safeguarded data portion, and determines who can substantially access a safeguarded document. The file key is used for enciphering/decoding the safeguarded data section, and is protected by the protection key. When contents in the safeguarded file are handled secretly, the file key is protected jointly not



only by the use permission key but also by the protection key regarding a user who tries to access the safeguarded file.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－218851
（Ｐ2003－218851Ａ）
(43)公開日　平成15年７月31日(2003.7.31)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード*(参考)
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　12/00	５３７Ａ	５Ｂ０１７
Ｇ０６Ｆ　12/00	５３７		５３７Ｈ	５Ｂ０８２
		12/14	３１０Ｋ	５Ｊ１０４
12/14	３１０		３２０Ｂ	
	３２０	Ｇ０９Ｃ　1/00	６６０Ｄ	

審査請求　未請求　請求項の数50　ＯＬ　（全 21 頁）　最終頁に続く

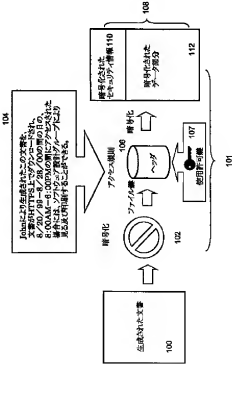
(21)出願番号　特願2002－359963(Ｐ2002－359963)
(22)出願日　平成14年12月11日(2002.12.11)
(31)優先権主張番号　３３９６３４
(32)優先日　平成13年12月12日(2001.12.12)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０７４８０４
(32)優先日　平成14年２月12日(2002.2.12)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　１５９５３７
(32)優先日　平成14年５月31日(2002.5.31)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　502448498
パーヴェイシヴ　セキュリティー　システムズ　インコーポレイテッド
Ｐｅｒｖａｓｉｖｅ　Ｓｅｃｕｒｉｔｙ　Ｓｙｓｔｅｍｓ，　Ｉｎｃ．
アメリカ合衆国　カリフォルニア州　94025　メンロー・パーク　ミドルフィールド・ロード　535　スイート・120
(74)代理人　100070150
弁理士　伊東　忠彦　（外３名）

最終頁に続く

(54)【発明の名称】　ディジタル資産を安全化する方法及び装置

(57)【要約】
【課題】　本発明は、常に、ディジタル資産を安全にし且つ保護する更に効果的な方法を提供することを目的とする。
【解決手段】　適切なアクセス権を有しても、安全化されたファイルが秘密である場合には、少なくともセキュリティ使用許可鍵が必要とされる。安全化されたファイルは、ヘッダと安全化されたデータ部分の２つの部分を有する。ヘッダは、アクセス規則、保護鍵及びファイル鍵をさす又は含むセキュリティ情報を含む。アクセス規則は、安全化されたデータ部分へのアクセスを容易にし、本質的に誰が安全化された文書をアクセスできるかを決定する。ファイル鍵が、安全化されたデータ部分を暗号化／復号するために使用され、保護鍵により保護される。安全化されたファイル内のコンテンツが秘密に扱われる場合には、ファイル鍵は、安全化されたファイルにアクセスしようとするユーザに関連する、使用許可鍵だけでなく保護鍵により共同で保護される。



【特許請求の範囲】

【請求項１】　電子データへの制限されたアクセスを提供するシステムにおいて、電子データは電子データ内のコンテンツへのアクセスを制御するフォーマットに構造化され、そのフォーマットは、

電子データ内のコンテンツへのアクセスを制御するセキュリティ情報を含むヘッダを有し、セキュリティ情報は少なくとも第１の鍵と第２の鍵を含み、第２の鍵は第１の鍵を暗号化するのに使用され、第２の鍵は暗号化されかつ暗号化された第２の鍵はアクセス規則により保護され

予め定められた暗号機構に従って第１の鍵で電子データを暗号化することにより発生された暗号化されたデータ部分を有し、且つ、

安全化されたファイルを発生するために、ヘッダが、暗号化されたデータ部分と統合される、フォーマット。

【請求項２】　アクセス規則は、安全化されたファイル内のアクセス制限は何かを表示するために、アプリケーション内に表示されることが可能である、請求項１に記載のフォーマット。

【請求項３】　アクセス規則は、更に暗号化され且つ、安全化された情報内に含まれる、請求項１に記載のフォーマット。

【請求項４】　アクセス規則は、記述的な言語で表現されている、請求項３に記載のフォーマット。

【請求項５】　記述的言語は、（ｉ）ＳＧＭＬ、（ｉｉ）ＨＴＭＬ、（ｉｉｉ）ＷＭＬ、（ｉｖ）ＸＡＣＭＬの１つのマークアップ言語である、請求項４に記載のフォーマット。

【請求項６】　第２の鍵は、予め定められた暗号機構に従って、第１の鍵を暗号化するのに使用される、請求項１に記載のフォーマット。

【請求項７】　暗号化された第１の鍵は、第１の鍵への制限的なアクセスを制御するセキュリティ使用許可情報により保護されている、請求項６に記載のフォーマット。

【請求項８】　セキュリティ使用許可情報は、第１の鍵は、第２の鍵と、安全化されたファイルアクセスしようとするユーザに関連する、使用許可鍵の両方とともにのみ取り出すことができるように、暗号化された第１の鍵の他の暗号である、請求項７に記載のフォーマット。

【請求項９】　セキュリティ使用許可情報は、第１の鍵は、第２の鍵と、安全化されたファイルアクセスしようとするユーザのアクセス権に対する特別なアクセスポリシーの成功的なテストと共にのみ取り出すことができるように、特別のアクセスポリシーに関連している、請求項７に記載のフォーマット。

【請求項１０】　第１の鍵は、暗号化されたデータ部分の復号だけでなく暗号化に使用されることが可能な、ファイル鍵であり、且つ、第２の鍵は、安全化されたファイルアクセスしようとするユーザに関連する、使用許可鍵と共に、ファイル鍵を保護するように指定された保護鍵である、請求項７に記載のフォーマット。

【請求項１１】　第２の鍵は、暗号化され且つアクセス規則により保護されている、請求項１０に記載のフォーマット。

【請求項１２】　アクセス規則は、さらに、暗号化され且つヘッダのセキュリティ情報内に含まれている、請求項１１に記載のフォーマット。

【請求項１３】　暗号化されたアクセス規則は、安全化されたファイルをアクセスしようとするユーザに関連するユーザ鍵で復号される、請求項１１に記載のフォーマット。

【請求項１４】　アクセス規則は、一旦復号されると、ユーザのアクセス権に対してテストされる、請求項１３に記載のフォーマット。

【請求項１５】　保護鍵は、アクセス規則に従って、ユーザがアクセス権を有するときにのみ取り出されることができる、請求項１４に記載のフォーマット。

【請求項１６】　ファイル鍵は、ユーザが、使用許可鍵を有するときにのみ取り出されることができる、請求項１５に記載のフォーマット。

【請求項１７】　セキュリティ使用許可情報は、安全化されたファイルの秘密レベルに関連し、秘密レベルは、最大の秘密から非秘密の範囲である、請求項７に記載のフォーマット。

【請求項１８】　１つの秘密レベルに指定された使用許可鍵は、その１つの秘密レベルの又はその１つの秘密レベルより低いすべての秘密レベルについて使用することができる、請求項１７に記載のフォーマット。

【請求項１９】　暗号化された第１の鍵は、第２の鍵を取り出さねばならないことなしに、更新されることができる、請求項１に記載のフォーマット。

【請求項２０】　電子データへの制限されたアクセスを提供するシステムにおいて、電子データは電子データ内のコンテンツへのアクセスを制御するフォーマットに構造化され、そのフォーマットは、

第１の鍵の暗号化版、第２の鍵の少なくとも１つの暗号化版、電子データ内のコンテンツへのアクセスを制御するアクセス規則を有するヘッダを有し、第２の鍵は対象であり且つ、十分なセキュリティ使用許可が外部的に供給されたときに、第１の鍵を取り出すだけでなく、第１の鍵の暗号化版を生成するのに使用され、

予め定められた暗号機構に従って第１の鍵で電子データを暗号化することにより発生された暗号化されたデータ部分を有し、且つ、

安全化されたファイルを発生するために、ヘッダが、暗号化されたデータ部分と統合される、フォーマット。

【請求項２１】　セキュリティ使用許可は、安全化されたファイルにアクセスしようとするユーザに関連する、

使用許可鍵である、請求項２０に記載のフォーマット。

【請求項２２】　記述的言語で表現されているアクセス規則は、誰が電子データ内のコンテンツにアクセスできるかを制御する、請求項２１に記載のフォーマット。

【請求項２３】　アクセス規則の少なくとも一部は、第２の鍵の暗号化版が復号されることができる前に、ユーザのアクセス権をテストするのに使用される、請求項２２に記載のフォーマット。

【請求項２４】　使用許可鍵は、１つの秘密レベルに対応し、且つ、安全化されたファイルが多くてその秘密レベルに分類されたときに、第１の鍵を取り出すために、第２の鍵と共に使用される、請求項２３に記載のフォーマット。

【請求項２５】　使用許可鍵は、１つの秘密レベルに対応し、且つ、安全化されたファイルがその秘密レベルに又は、その秘密レベルより低い全てのレベルに分類されたときに、第１の鍵を取り出すために、第２の鍵と共に使用される、請求項２３に記載のフォーマット。

【請求項２６】　暗号化されたデータ部分は、複数のセグメントを有し、各々は電子データの１つのブロックを暗号化することから発生される、請求項２０に記載のフォーマット。

【請求項２７】　ブロックのブロックサイズは定数である、請求項２６に記載のフォーマット。

【請求項２８】　定数は、予め定められた暗号機構内で定義されたブロックサイズの倍数である、請求項２７に記載のフォーマット。

【請求項２９】　電子データへの制限されたアクセスを提供するシステムにおいて、電子データは電子データ内のコンテンツへのアクセスを制御するフォーマットに構造化される、そのフォーマット内の電子データを安全化する方法であって、その方法は、
予め定められた暗号機構に従って、第１の鍵で電子データを暗号化することにより、暗号化されたデータ部分を発生し、
電子データが秘密でない場合には、第２の鍵で第１の鍵を暗号化し、
電子データが秘密である場合には、使用許可鍵とともに、第２の鍵で第１の鍵を暗号化し、
第２の鍵の暗号化版を発生するために第２の鍵を暗号化し、
第２の鍵の暗号化版を保護するために、アクセス規則を適用し、
安全化されたファイルを生成するために、ヘッダを暗号化されたデータ部分と統合し、ヘッダは、暗号化された第１の鍵、暗号化された第２の鍵及びアクセス規則を含む、方法。

【請求項３０】　アクセス規則は、電子データのコンテンツにアクセスしようとするユーザに関連する認証されたユーザ鍵でのみ復号されることができる、請求項２９に記載の方法。

【請求項３１】　電子データが秘密である場合には、使用許可鍵とともに、第２の鍵で第１の鍵を暗号化することは、
第１の鍵の初期暗号化版を生成するために第２の鍵で第１の鍵を暗号化し、
第１の鍵の暗号化版を生成するために、使用許可鍵で第１の鍵の初期暗号化版を暗号化する、請求項２９に記載の方法。

【請求項３２】　電子データが秘密である場合には、使用許可鍵とともに、第２の鍵で第１の鍵を暗号化することは、
第１の鍵の初期暗号化版を生成するために使用許可鍵で第１の鍵を暗号化し、第１の鍵の暗号化版を生成するために、第２の鍵で第１の鍵の初期暗号化版を暗号化する、請求項２９に記載の方法。

【請求項３３】　使用許可鍵は、第１の鍵を取り出すために使用許可鍵が使用されるのは、どの秘密の安全化されたファイルかを決定する、秘密レベルに対応する、請求項２９に記載の方法。

【請求項３４】　秘密レベルは、最大の秘密から非秘密の範囲である、請求項３３に記載の方法。

【請求項３５】　使用許可鍵の秘密レベルに又は使用許可鍵の秘密レベルよりも低く分類された安全化されたファイル内の第１の鍵を取り出すために、アクセス規則が、電子データ内の内容にアクセスしたいユーザのアクセス権に対して成功的に測定された場合には、使用許可鍵は、第２の鍵と共に使用されることができる、請求項３４に記載の方法。

【請求項３６】　アクセス規則は、記述的言語で表現される、請求項３５に記載の方法。

【請求項３７】　記述的言語は、マークアップ言語である、請求項３６に記載の方法。

【請求項３８】　マークアップ言語は、（ｉ）ＳＧＭＬ、（ｉｉ）ＨＴＭＬ、（ｉｉｉ）ＷＭＬ、及び（ｉｖ）ＸＡＣＭＬのうちの１つである、請求項３７に記載の方法。

【請求項３９】　第２の鍵の暗号化版を発生するために第２の鍵を暗号化することは、
電子データを安全化したいユーザに関連する公開ユーザ鍵を取得し、且つ、
予め定められた暗号機構に従って、公開ユーザ鍵を使用して、第２の鍵を暗号化する、請求項２９に記載の方法。

【請求項４０】　第２の鍵の暗号化版は、秘密ユーザ鍵が認証されている場合には、ユーザに関連する秘密ユーザ鍵で復号される、請求項３９に記載の方法。

【請求項４１】　電子データへの制限されたアクセスを提供するシステムにおいて、電子データは電子データ内のコンテンツへのアクセスを制御するフォーマットに構

造化される、その電子データにアクセスする方法であって、その方法は、
電子データにアクセスしたいユーザに関連する認証されたユーザ鍵を取得し、
ユーザが適切なアクセス権を有するかを決定するために、フォーマット内に埋めこまれたアクセス規則を取り出し、
ユーザが電子データにアクセスすることが許されている場合には、第２の鍵を取り出し、
電子データ内のコンテンツが秘密である場合には、
ユーザに関連する使用許可鍵を取得し、
第１の鍵を最後に取り出すために、第２の鍵と使用許可鍵とを使用し、
電子データ内のコンテンツが秘密でない場合には、
第１の鍵を取り出すために、第２の鍵を使用し、
第１の鍵を使用して、電子データの暗号化版をまず暗号化されたデータ部分を復号する、方法。

【請求項４２】　アクセス規則も、暗号化される、請求項４１に記載の方法。

【請求項４３】　ユーザが適切なアクセス権を有するかを決定するために、フォーマット内に埋めこまれたアクセス規則を取り出すことは、
認証されたユーザ鍵でアクセス規則を復号し、且つ、
ユーザのアクセス権がアクセス規則内であるかどうかをテストする、ことを含む、請求項４２に記載の方法。

【請求項４４】　アクセス規則は、記述的言語で表現され且つ、誰が及び／又はどのように電子データをアクセスすることができるかを制御する、請求項４３に記載の方法。

【請求項４５】　ユーザが電子データにアクセスすることが許されている場合には、第２の鍵を取り出すことは、ユーザが電子データにアクセスすることが許されていると決定された後に、認証されたユーザ鍵で復号される第２の鍵を復号することを含む、請求項４２に記載の方法。

【請求項４６】　第１の鍵を最後に取り出すために、第２の鍵と使用許可鍵とを使用することは、第１の鍵の暗号化版を復号するために、第２の鍵と使用許可鍵を連続して使用することにより、第１の鍵を取得する、請求項４１に記載の方法。

【請求項４７】　第１の鍵を最後に取り出すために、第２の鍵と使用許可鍵とを使用することは、第１の鍵の暗号化版を復号するために、使用許可鍵と第２の鍵を連続して使用することにより、第１の鍵を取得する、請求項４１に記載の方法。

【請求項４８】　この方法は、ユーザがそれから電子データにアクセスしようとするクライアントマシン内で実行される、請求項４１に記載の方法。

【請求項４９】　電子データへの制限されたアクセスを提供するコンピューティングシステム内で実行されるソフトウェアプロダクトであって、電子データは、電子データ内のコンテンツへのアクセスを制御するフォーマットに構造化され、そのソフトウェアプロダクトは、
予め定められた暗号機構に従って、第１の鍵で電子データを暗号化することにより、暗号化されたデータ部分を発生するプログラムコードと、
電子データが秘密でない場合には、第２の鍵で第１の鍵を暗号化するプログラムコードと、
電子データが秘密である場合には、使用許可鍵とともに、第２の鍵で第１の鍵を暗号化するプログラムコードと、
第２の鍵の暗号化版を発生するために第２の鍵を暗号化するプログラムコードと、
第２の鍵の暗号化版を保護するために、アクセス規則を適用するプログラムコードと、
安全化されたファイルを生成するために、ヘッダを暗号化されたデータ部分と統合するプログラムコードとを有し、ヘッダは、暗号化された第１の鍵、暗号化された第２の鍵及びアクセス規則を含む、ソフトウェアプロダクト。

【請求項５０】　電子データへの制限されたアクセスを提供するコンピューティングシステム内で実行されるソフトウェアプロダクトであって、電子データは電子データ内のコンテンツへのアクセスを制御するフォーマットに構造化され、そのソフトウェアプロダクトは、
電子データにアクセスしたいユーザに関連する認証されたユーザ鍵を取得するプログラムコードと、
ユーザが適切なアクセス権を有するかを決定するために、フォーマット内に埋めこまれたアクセス規則を取り出すプログラムコードと、
ユーザが電子データにアクセスすることが許されている場合には、第２の鍵を取り出すプログラムコードと、
電子データ内のコンテンツが秘密である場合には、
ユーザに関連する使用許可鍵を取得するプログラムコードと、
第１の鍵を最後に取り出すために、第２の鍵と使用許可鍵とを使用するプログラムコードと、
電子データ内のコンテンツが秘密でない場合には、
第１の鍵を取り出すために、第２の鍵を使用するプログラムコードと、
第１の鍵を使用して、電子データの暗号化版を表す暗号化されたデータ部分を復号するするプログラムコードと、を有するソフトウェアプロダクト。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この出願は、２００２年２月１２日に出願され且つ発明の名称”（アクセス制御のための安全化データフォーマット）Ｓｅｃｕｒｅｄ Ｄａｔａ Ｆｏｒｍａｔ ｆｏｒ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ”の、米国特許出願番号１０／０７４，８０４の

部分継続出願であり、参照によりここに込みこまれる。この出願は、２００１年１２月１２日に出願された、発明の名称”（全面的に広まるセキュリティシステム）ＰＥＲＶＡＳＩＶＥ　ＳＥＣＵＲＩＴＹ　ＳＹＳＴＥＭＳ”の、米国仮特許出願番号６０／３３９，６３４の利益を請求し、そして、参照によりここに組み込まれる。この出願は、発明の名称”（安全化されたディジタル資産へのアクセス権の評価）Ｅｖａｌｕａｔｉｏｎ　ｏｆ　Ａｃｃｅｓｓ　Ｒｉｇｈｔ　ｔｏ　Ｓｅｃｕｒｅｄ　Ｄｉｇｉｔａｌ　Ａｓｓｅｔｓ”の、米国特許出願番号１０／１２７，１０９のにも関連し、参照によりここに込みこまれる。

【０００２】本発明は、企業環境内のデータの保護の分野に関連し、特に、ディジタル資産（例えば、電子データ）を安全化するための方法と装置に関連する。

【０００３】

【従来の技術】歴史的に、インターネットは最も速く成長する通信媒体である。この成長とそれが得らる簡単なアクセスは、公共と私的セクターの両方で、進んだ情報技術を使用する機会が非常に向上されている。これは、企業と個人に相互動作とデータの共有の予想できない機会を提供する。しかしながら、インターネットにより提供される優位点は、情報の秘密性と完全性の危険の非常に大きな要素が付随している。インターネットは、相互に接続されたコンピュータと電子装置の広く開放された、公共的な且つ国際的なネットワークである。適切な安全な手段がなければ、許可されていない者又は機械が、インターネットをわたって通信する情報を傍受し、且つ、公共により一般的にはアクセスされない、インターネットに相互接続されたコンピュータ内に蓄積された専有の情報へアクセスさえする。

【０００４】インターネットをわたって送られる専有の情報を保護し且つ専有の情報を担うコンピュータを制御する目的に多くの努力が進歩している。暗号化は人々に、電子世界に、物理的な世界で見つかった信頼を担うことを許し、これは、人々が、ごまかしや詐欺の心配無しに電子的に取引をすることを許している。毎日何十万人もが、電子メール、電子商取引（インターネット上で行われる取引）、ＡＴＭマシン、又は、携帯電話のように、電子的に相互に作用する。電子的に伝送された情報の知覚的な増加は、暗号の増加された信頼性を導いている。

【０００５】インターネットをわたって送られる専有の情報を保護する進行中の努力の１つは、インターネット上の２つの通信するコンピュータの間の私的通信セッションを安全化するために、１つ又はそれ以上の暗号化技術を使用することである。暗号化技術は、通信チャネルを盗み聞きする者に情報の内容を開示すること無しに、不安な通信チャネルをわたり情報を伝送する方法を提供する。暗号化技術内の暗号処理を使用して、１つのパーティーが、許可されていない第３のパーティーのアクセスから、送信中のデータの内容を保護することができ、さらに、意図されたパーティーは対応する復号処理を使用して、データを読むことができる。

【０００６】ファイアーウォールは、他のネットワークのユーザから、プライベートネットワークの資源を保護する、他のセキュリティ手段である。しかしながら、専有の情報への多くの未許可のアクセスが、外側からでは無く内側から発生することが、報告されている。内側からの幾つかの未許可のアクセスを得る例は、制限された又は専有の情報が、そうするとは予想されていない組織内の誰かによりアクセスされるときである。インターネットの開放的な性質により、契約情報、顧客データ、エグゼクティブ通信、製品仕様、及び他の秘密及び占有知的財産のホストが、おそらく保護された周囲の中又は外側から、未許可のユーザによる不適切なアクセス又は使用に対して、利用できるまま且つ無防備なまま残る。

【０００７】会計検査院（ＧＡＯ）からの政府報告は、”米国商務省内の７つの組織での重大な且つ全面的に広まるコンピュータセキュリティの弱さ、組織を通しての広まったコンピュータセキュリティの弱さは、機関の最も敏感ないくつかのシステムの完全性を非常に危険にさらしている”と詳細に述べている。さらに、それは、”容易く利用できるソフトウェア及び一般的な技術を使用して、商務省内部からそしてインターネットを通して遠隔的にこの両方から、敏感な商務省システムを貫通することができることを示し”且つ、”商務省内と外部の両方の個人は、これらのシステムに未許可のアクセスができ、且つ敏感な経済的、財政的、人事的及び秘密の事業データを、読み、コピーし、修正し且つ消去することができる”。報告は更に、侵入者は部門の使命に重要なシステムの動作を混乱させることができると結んでいる。

【０００８】

【発明が解決しようとする課題】実際には、多くの企業と組織は、専有の情報を保護する効果的な方法を渡している。典型的には、企業と組織は、保護を設けるために、ファイアーウォール、仮想プライベートネットワーク（ＶＰＮ）及び侵入検知システム（ＩＤＳ）を配備している。不運なことに、これらの種々のセキュリティ手段は、プライベートネットワーク内にある専有の情報を信頼性をもって保護するのに不充分であることが分かった。例えば、その中から敏感な文書にアクセスするためにパスワードに依存することは、しばしば、数文字のパスワードが漏れ又は検出されたときに、セキュリティの裂け目を発生する。従って、常に、ディジタル資産を安全にし且つ保護する更に効果的な方法を提供することが必要である。

【０００９】

【課題を解決するための手段】このセクションは、本発

明は、幾つかの特徴の概要を説明する目的と、幾つかの適する実施例を簡単に説明することを目的とする。単純化又は省略は、このセクションの目的を曖昧にすることを避けるためになされる。そのような単純化又は省略は、本発明の範囲を制限するものではない。

【００１０】本発明は、常にディジタル資産に全面的に広まるセキュリティ（又は、安全性）を提供する且つとりわけ企業環境で安定である処理、システム、構造及びソフトウェアプロダクトに関連する。一般的には、全面的に広まるセキュリティは、ディジタル資産が常に安全にされ、そして、適切なアクセス権を有する認証されたユーザによってのみアクセスでき、且つ、幾つかの場合には、適切なセキュリティ使用許可を意味し、ここで、ディジタル資産は、制限はされないが、種々の形式の文書、マルチメディアファイル、データ、実行可能なコード、画像及びテキストを含む。本発明の１つの特徴に従って、ディジタル資産は、許可されたアクセス権を有する者のみがアクセスできる安全な形式である。適切なアクセス権を有するときでさえ、安全化されたファイルが秘密であるときには、少なくともセキュリティ使用許可鍵が、正しいセキュリティ使用許可を有する者が最後に秘密の安全化されたファイル内のコンテンツにアクセスできることを保証するために、必要である。

【００１１】本発明の他の特徴では、安全化されたファイルのフォーマットは、安全化された情報は、常に、安全化されたファイルと共に存在し、又は、ファイル内のポインタにより示される、ように設計されている。一実施例に従って、安全化されたファイル又は、安全化された文書は、ヘッダーと呼ばれる付属部分と、暗号化された文書又はデータ部分の、２つの部分を有する。ヘッダは、アクセス規則を指す又は含むセキュリティ情報、保護鍵及びファイル鍵を含む。アクセス規則は、暗号化されたデータ部分への制限されたアクセスを容易にし、且つ本質的に、誰／どのように及び／又は、いつ／どこで、安全化された文書がアクセスされうるかを決定する。ファイル鍵は、暗号化されたデータ部分を暗号化／復号するのに使用され、そして、保護鍵により保護される。安全化されたファイル内のコンテンツが秘密である場合には、ファイル鍵は、安全化されたファイルをアクセスしようとするユーザに関連するセキュリティ使用許可鍵だけでなく、保護鍵により共同で保護される。この結果、適切なアクセス権を有する者のみが、暗号化されたデータ部分を復号するファイル鍵を取得するために、保護鍵、共同でセキュリティ使用許可鍵を取り出すことが許される。

【００１２】本発明のさらに他の特徴では、セキュリティ使用許可鍵は、ユーザのセキュリティアクセスレベルに従って、発生され且つ割当てられる。セキュリティ使用許可鍵は、最大の秘密から非秘密の範囲を取る。ユーザがあるセキュリティ又は秘密レベルを有する秘密の安全化されたファイルにアクセスする必要がある場合には、そのセキュリティレベルを有する対応するセキュリティ使用許可鍵がそのために割当てられる。一実施例では、あるセキュリティレベルを有するセキュリティ使用許可鍵は、鍵がそのセキュリティレベルに又はそのセキュリティレベルより低く分類された安全化されたファイルをアクセスするのに使用されるように、設定される。この結果、ユーザは、１つのセキュリティ使用許可鍵のみを有する必要がある。更に、本発明の他の特徴では、対応するセキュリティ使用許可鍵が要求されているときには、複数の補助鍵が供給される。セキュリティ使用許可鍵は、要求され、決定されたセキュリティレベルに従って発生され、且つ対応するセキュリティレベル又は秘密レベルで秘密扱いされる安全化されたファイルへのアクセスを容易にすることができるものである。補助セキュリティ使用許可鍵は、それぞれ対応するセキュリティレベル又は秘密レベルより低く秘密扱いされた、安全化されたファイルへのアクセスを容易にするために発生された鍵である。実行に依存して、セキュリティ使用許可鍵は更に、セキュリティ使用許可鍵のセキュリティレベルを増加させる、生物測定学的な情報確認又は、第２のパスワードのような、第２の認証により保護される。

【００１３】実行と応用に依存して、本発明は、クライアントマシン又はサーバマシン内で実行され又は採用されうる。典型的には、安全化されたファイルへのユーザのアクセス権（即ち、アクセス権）が、クライアントマシン内で局所的に決定される場合には、本発明は、好ましくはクライアントマシン内で走るオペレーティングシステム内で、ローカルに動作するように設定された実行可能なモジュールとして実行されうる。安全化されたファイルへのユーザのアクセス権が、サーバマシン内で遠隔的に決定される場合には、本発明は、サーバマシンと、クライアントマシン内で動作するように設定された実行可能なモジュールとして実行されうる。

【００１４】本発明の他の特徴及び優位点は、添付の図面と共に、実施例の以下の詳細な説明から明らかとなろう。

【００１５】本発明のこれらの特徴及び優位点は、以下の説明、請求の範囲、添付の図面と共に、からより理解されよう。

【００１６】

【発明の実施の形態】本発明は、電子データ又は、ディジタル資産を安全化する処理、システム、方法及びソフトウェアプロダクトに関連する。本発明の１つの特徴に従って、安全化されたファイルは幾つかの階層的なセキュリティレベルで分類される。安全化された秘密扱いのファイルにアクセスするために、ユーザ鍵に加えて、ユーザは２つの相補的な概念、安全化された秘密扱いのファイル内の情報の”知る必要がある”と”敏感なレベル”に基づいている、使用許可鍵が割当てられる。本発

明のたの特徴に従って、ディジタル資産は、１つは暗号化された部分と他は暗号化されたデータ部分への制限的なアクセスを制御するセキュリティ情報を含むヘッダの２つの部分を含む形式である。セキュリティ情報は、適切なアクセス特権又はアクセス権を有する者のみが暗号化されたデータ部分をアクセスできることをを保証するために、種々の暗号化鍵と共にアクセス規則を採用する。

【００１７】本発明は、多くの優位点、利益、及び、特徴を有する。それらの１つは、常に保護されることが求められるディジタル資産に全面的に広まるセキュリティを提供することのできると考えられる機構である。他の１つは、ディジタル資産は、十分なセキュリティ使用許可レベルだけでなく適切なアクセス権を有する者のみがディジタル資産内の情報にアクセスできるようにに提示されることである。本発明の他の優位点、利益、特徴は、ここに提供される本発明の詳細な説明により、当業者には容易に理解されうる。

【００１８】以下の説明では、多くの特定の詳細が本発明の徹底的な理解のために述べられる。しかしながら、本発明は、特定の詳細無しに実行されうることは、当業者には明らかである。ここの説明と表現は、当業者が他の当業者にその仕事の実体を伝えるのに最も効果的な一般的な手段である。他の実体では、本発明を不用に曖昧にすることを避けるために、既知の方法、手順、構成要素、及び回路が、詳細に説明されない。

【００１９】ここで、”一実施例”又は、”１つの実施例”と呼ぶのは、特定の幹徴、構造、又は、実施例と共に説明される特徴は、本発明の少なくとも１つの実施例に含まれることを意味する。明細書の種々の場所で現れるフレーズ”一実施例では”は、全て同じ実施例を参照する必要はなく、又は、他の実施例と相互に排他的な別の又は他の実施例を参照する必要はない。更に、本発明の１つ又はそれ以上の実施例を表す処理フロー又は図は内のブロックの順序は特定の順序を固有に示すものではまく又は、本発明の制限することを意味するものでもない。

【００２０】本発明の実施例は、図１－６を参照して説明される。しかしながら、これらの図面に関するここに与えられる詳細な説明は、例示目的であり、本発明は、これらの制限的な実施例を超えることは、当業者には、容易く理解される。

【００２１】一般的には、エンティティのために製作者により作成されるコンテンツは、製作者又はエンティティに属する知的財産である。企業では、どのような情報又は知的財産もコンテンツであり、しかし、”コンテンツ”の代わりに”情報”と一般的には、呼ばれる。いずれの場合にも、コンテンツ又は情報はそのフォーマットと独立であり、それは、印刷物又は、電子文書でもよい。ここで使用されるように、コンテンツ又は情報は、ディジタル資産とも呼ばれる電子データの形式で存在する。電子データの表現は、制限はされないが、種々の形式の文書、マルチメディアファイル、ストリーミングデータ、ダイナミック又はスタティクデータ、実行可能なコード、画像及びテキストを含んでもよい。

【００２２】電子データ内のコンテンツを未許可のアクセスから防ぐために、電子データは典型的には、演繹的な知識無しにはほぼ読み出せない形式で格納される。その目的は、電子データにアクセスできる者でも、それが意図されていない人からコンテンツを隠して保つことにより、プライバシーを保証することである。演繹的な知識の例は、制限はされないが、パスワード、秘密のフレーズ、生物測定学的な情報又は、１つ又はそれ以上の鍵である。

【００２３】図１は、本発明の一実施例に従って、生成された文書１００を安全にする図を示す。安全化されたファイル１０８を生成するの目的の１つは、文書１００内のコンテンツが適切なアクセス権を有する許可されたユーザにのみアクセスされ又は、取り出されることができることを保証することである。ここで、使用するように、ユーザは、人間のユーザ、ソフトウェアエージェント、ユーザのグループ又は、そのメンバ、装置及び／又はアプリケーションを意味する。安全化された文書にアクセスする必要のあるユーザ、ソフトウェアアプリケーション又は、エージェントは、しばしば、処理を進めるために、安全化された文書にアクセスする必要がある。従って、特に述べない限り、ここで使用される”ユーザ”は、人間に関係する必要なない。

【００２４】文書１００が生成され、編集され又は、アプリケーション又はオーサリングツール（例えば、マイクロソフトワード（登録商標））により開かれた後に、”保存”、”名前をつけて保存”又は、”閉じる”のようなコマンドの活性化、又は、オペレーティングシステム、アプリケーション自身又は、是器されたアプリケーションによる自動的な保存に際し、生成された文書１００は安全化処理１０１を受ける。安全化処理１０１は、暗号化処理１０２で開始する、即ち、生成された又はメモリに書きこまれている文書１００は、ファイル鍵（即ち、暗号化鍵）を使用して暗号器（例えば、暗号化処理）により暗号化される。言い替えると、暗号化されたデータ部分１１２は、ファイル鍵なしでは開けることができない。文書１００又は結果の安全化されたファイル１０８内のコンテンツへのアクセスを制御する目的で、ファイル鍵又は鍵は、暗号化と復号で同じ又は異なる鍵でもよく、そして、セキュリティ情報の一部としてヘッダ１０６に含まれる又は指示される。ファイル鍵は、一旦得られると、コンテンツを明らかにするのに、暗号化されたデータ部分１１２を復号するのに使用できる。

【００２５】認可されたユーザ又は認可されたグループ

のメンバのみが安全化されたファイル１０８にアクセスできることを保証するために、文書１００についてのアクセス規則１０４の組みが、受信され又は生成されそしてヘッダ１０６と関連させられる。一般的には、アクセス規則１０４は、誰が及び／又はどのように、一旦安全化された文書１００をアクセスできるかを決定し又は調整する。ある場合には、アクセス規則１０４は、いつ及び／又はどこで、文書１００をアクセスできるかを決定し又は調整する。更に加えて、安全化されたファイル１０８が秘密に扱われる場合には、セキュリティ使用許可情報１０７がヘッダ１０６に追加される。一般的には、セキュリティ使用許可情報１０７は、安全化されたファイル１０８内のコンテンツにアクセスしようとするユーザのアクセス特権のレベル又は、セキュリティレベルを決定するのに使用される。例えば、安全化されたファイルは、”極秘”、”機密”、”秘密”及び”非秘密”に分類されうる。

【００２６】一実施例に従って、セキュリティ使用許可情報１０７は、使用許可鍵とここでは呼ばれる他の鍵を用いる、ファイル鍵の暗号化の他のレイヤを含む。認可されたユーザは、認可されたユーザ鍵とファイル鍵を取り出す適切なアクセス権に加えて、適切なセキュリティレベルの使用許可鍵を有する必要がある。ここで使用されるように、ユーザ鍵又は、グループ鍵は、認可されたユーザに割当てられた暗号鍵であり、そして、安全化されたファイルにアクセスする、又は、ファイルを安全化する、又は、安全化されたファイルを生成するのに使用される。認可されたユーザによるそのようなユーザ鍵を得る詳細は、米国特許出願番号１０／０７４，８０４に記載されている。

【００２７】他の実施例に従って、セキュリティ使用許可情報１０７は、ファイル鍵を保護する特別のアクセス規則の組みを含む。ファイル鍵の取り出しは、ユーザがアクセス規則測定を通過することを要求する。ユーザのアクセス権は１つ又はそれ以上のシステムパラメータ（例えば、ポリシー）により制御されているので、アクセス規則測定は、対応するユーザ鍵と共にファイル鍵を取り出すために、ユーザが十分なアクセス権を有するかどうか決定する。以下の詳細な説明では、当業者は、セキュリティ使用許可情報１０７の他の形式も可能であることは理解されよう。規定されていなければ、以下の説明は、１つ又はそれ以上の使用許可情鍵での暗号化の他のレイヤであるセキュリティ使用許可情報１０７に基づいている。

【００２８】セキュリティ使用許可情報１０７に従って、ユーザは、ユーザに割当てられたおそらく信頼のレベルに基づく階層的なセキュリティ使用許可レベルを割当てられる。信頼のレベルは、ある一人のユーザが他の者よりも更に信頼があることを暗示し、そして、これゆえに更に信頼されるユーザは、更なる秘密のファイルにアクセスしてもよい。実行に依存して、信頼のレベルは、プロジェクト又は組織バックグランドチェック内のユーザの仕事の責任又はユーザの役割、心理プロファイル又は、サービスの長さ等に基づいてもよい。どの場合にも、ユーザに割当てられた信頼のレベルは、ユーザがアクセス規則によりファイルにアクセスすることを許されている場合でさえも、秘密に扱われる安全化されたファイルにアクセスするには、適切なセキュリティ使用許可を有する必要があるように、ユーザのアクセス権の追加の特徴を増加する。

【００２９】以下に更に詳細に説明するように、ユーザのセキュリティ使用許可が許さない限り、安全化された秘密に扱われるファイル（即ち、安全化された且つ秘密に扱われるファイル）は、ユーザが認証されたユーザ（又は、グループ）鍵を有し且つ安全化された秘密に扱われるファイル内のアクセス規則により許される場合でさえ、アクセスされない。一実施例では、ユーザのセキュリティ使用許可のレベルが、１つ又はそれ以上のそれに割当てられた使用許可鍵により決定される。一般的には、使用許可鍵は、ユーザが”極秘”と分類された安全化されたファイルにアクセスすることを許し、同じ使用許可鍵は、ユーザが、”機密”又は”秘密”のような、より安全度の低い、全ての安全化されたファイルにアクセスすることを許し、ここでは、ユーザは、ファイル内のアクセス規則により許された、適切なアクセス権を有すると仮定される。一実施例では、使用許可鍵は更に、生物測定学的な情報確認及び第２のパスワードにような、第２の認証により更に安全化される。言い替えると、ユーザが追加の情報を供給しなければ、使用許可鍵は、認証的にログインすると、自動的にユーザに開放されず又は、ユーザについて活性化されない。

【００３０】一般的には、ヘッダはファイル構造であり、好ましくは小サイズで、且つ結果の安全化された文書についてのセキュリティ情報を含む又は、おそらくリンクする。正確な実行に依存して、セキュリティ情報は全体的に、ヘッダ内に含まれ、又は、ヘッダ内に含まれているポインタにより指示される。実施例に従って、アクセス規則１０４は、セキュリティ情報の一部として、ヘッダ１０６内に含まれる。セキュリティ情報は、更に、ファイル鍵及び／又は１つ又はそれ以上の使用許可鍵を含み、ある場合には、オフラインアクセス許可（例えば、アクセス規則内）は、認可されたユーザにより要求されるそのようなアクセスである。セキュリティ情報は、そして、暗号化されたセキュリティ情報１１０を発生するために認可されたユーザに関連するユーザ鍵で、暗号器（即ち、暗号化／復号機構）により暗号化される。暗号化されたヘッダ１０６は、それに他の情報は付加されない場合には、結果の安全化されたファイル１０８を発生するために、暗号化されたデータ部分１１２に添付され又は統合される。好ましい実施例では、安全

化されたファイルの安全化された性質の素早い検出を容易にするために、ヘッダは、暗号化された文書（データ部分）の先頭に配置される。そのような配置の優位点の１つは、アクセスアプリケーション（即ち、オーサリング又は、視聴ツール）に、許されている場合には、ヘッダを復号するために、（適切であると説明されるべき）文書安全化モジュールをすぐに活性化することを、可能とすることである。それにも関わらず、暗号化されたヘッダ１０６が暗号化されたデータ部分１１２に統合されるということに関して制限はない。

【００３１】暗号化器は多くの利用できる暗号化／復号アルゴリズムの１つに基づいて、実行されると理解される。暗号化と復号は、一般的には、鍵と呼ばれる、ある秘密情報を使用することを要求する。ある暗号化機構では、暗号化と復号で同じ鍵が使用され、そして、他の機構では、暗号化と復号で使用される鍵が異なる。いずれの場合にも、予め定められた暗号化（即ち、暗号。復号）機構に従って、鍵で暗号化される。そのような機構の例は、制限はされないが、データ標準（Ｄａｔａ　Ｅｎｃｒｉｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）アルゴリズム（ＤＥＳ）、Ｂｌｏｗｆｉｓｈブロック暗号化及びＴｗｏｆｉｓｈ暗号化を含む。従って、本発明の動作は、それらの通常に使用される暗号化／復号機構の選択に制限されない。効果的で且つ信頼性のあるいずれの暗号化機構が使用されてもよい。したが特定の機構の詳細は、本発明の特徴を曖昧にするのでここでは更なる説明は行わない。

【００３２】本質的には、安全化された文書１０８は、暗号化されたデータ部分１１２（即ち文書自身の暗号化版）及び、安全化されたファイル１０８についてのセキュリティ情報を示すヌは含むヘッダ１１０の、２つの部分を含む。暗号化されたデータ部分１１２内のコンテンツにアクセスするために、暗号化されたデータ部分１１２を復号するために、ファイル鍵を得る必要がある。ファイル鍵を得るために、ユーザヌはグループ鍵を得るために認証される必要があり且つ、ユーザのアクセス特権に（即ち、アクセス権）対して、セキュリティ情報内の少なくともアクセス規則が測定される、アクセステストを通過する必要がある。安全化されたファイルが秘密である場合には、更に、ユーザに関するセキュリティレベル使用許可を要求する。一般的には、ユーザのセキュリティ使用許可レベルは、ファイル鍵が取り出せる前に、十分に高くなければならない。代わりに、アクセス規則の一部は、表示アプリケーションヌはマークアップ言語インタープリター（例えば、ブラウザ）内で、安全なファイルの埋めこまれたアクセス許可を見るのと同様に、認可された又は認可されないユーザについて、暗号化されないまま残される。

【００３３】図２Ａは、本発明の一実施例に従って、２つの異かれたアクセス機構と呼ばれる図２００を示す。安全化されたファイル２０１をアクセスするために、ユーザは、安全化されたファイル２０１に埋めこまれている、アクセス規則２０４に対して測定されるべき、”知る必要がある”条件２０２に基づいて、アクセス権を有する必要がある。安全化されたファイル２０１が秘密である場合には、ユーザは、セキュリティ使用許可レベル２０６に対して測定される（例えば、１つヌはそれ以上の使用許可鍵）より高いセキュリティ使用許可レベル２０６を有しなければならない。言い替えると、安全化された秘密に扱われるファイルがアクセスされることができる前に、２つの適切な鍵が”挿入される”少なくとも２つの鍵穴２１０がある。

【００３４】図２Ｂは、本発明の一実施例に従って、適切なセキュリティ使用許可レベル（即ち、使用許可鍵）を認可する処理のフローチャート２２０を示す。この処理２２０は、使用許可鍵の要求で開始される。実行に依存して、処理２２０は、おそらく、とりわけ企業環境内で又は、ユーザにより使用されるローカルクライアントマシンとそのマシンの組合せ内で、全ての安全化されたファイルにアクセス制御管理を提供する、機械（例えば、中央サーバ、ローカルサーバ又は、クライアントマシン）の中で実行される。

【００３５】２２２では、処理２２０は使用許可鍵の要求を待つ。安全化されたファイルは秘密又は、非秘密であるということが記述される。ユーザが秘密扱いの安全化されたファイルにアクセスする必要があるときには、そのような要求が処理２２０を活性化するために供給される。一般的には、要求は、特定のユーザ又はグループ内のあるメンバに関連する。２２４で、ユーザについてのアカウントがあれば、ユーザについての対応するアカウントが取り出される。アカウントが利用できない場合には、それに従って、アカウントが開かれねばならない。代わりに、処理２２０は、あるセキュリティ又は秘密レベルで安全化されたファイルにアクセスする知る必要のある基準を有する、ユーザについての適切なアカウントを開く処理の一部でもよい。実行に依存して、対応するアカウント情報は、ユーザ名又は識別子、メンバーシップ情報、指定されたアクセス権及び（しばしば秘密鍵と公開鍵の対の）対応するユーザ鍵を含みうる。２２６で、ユーザについてのセキュリティレベルが決定され、これは、通常は必要性によりなされる。例えば、企業の重役は、最も高いセキュリティ使用許可レベルが割当てられ、そして、受け付けは、最も低いセキュリティ使用許可レベルが割当てられる。一旦セキュリティレベルが決定されると、使用許可鍵が２２８で発生される。

【００３６】図２Ｃを参照すると、本発明の一実施例に従って、使用許可鍵を発生する図２４０が示されている。鍵発生器２４４は、鍵としての英数字又は２値番号のシーケンスを発生するために、図２Ｂの２２６で決定されたセキュリティレベルを制御する１つヌはそれ以上

のパラメータ２４２を受信する。秘密鍵暗号システム又は、公開鍵暗号システムのいずれにせよ、鍵発生のためのランダム数の良好なソースが必要である。良好なソースの主な特徴は、潜在的な敵により未知の又は予測でさない数を発生することである。例えば、ランダム数が物理的なプロセスから得られる、そのような数を発生する多くの方法がある。他のアプローチは、ランダムシードによりフィードされる擬似ランダム数発生器を使用することである。いずれの場合にも、入力２４２に応じて、発生器２４４は適切なセキュリティレベルの使用許可鍵を発生するように構成される。一実施例では、鍵発生器２４４は、異なる長さ又は形式の鍵２４６を発生し、鍵２４６の各々は、レベル１（最高のセキュリティ）、レベル２、．．．．レベルＮ（最低のセキュリティ）のようなセキュリティレベルに対応する。他の実施例では、鍵発生器２４４により発生された鍵２４６の各々は、セキュリティを示す署名と共に埋めこまれる。使用許可鍵のセキュリティレベルを規定する他の方法も可能である。あるセキュリティレベルを有する各使用許可鍵が同じセキュリティレベルで分類された安全化されたファイルのみをアクセスするように、実行することは可能であるが、より高いセキュリティレベルを有する使用許可鍵が、より低いセキュリティレベルに分類された安全化されたファイルをアクセスすることを許すことが、好ましい。言い替えると、レベル１の使用許可鍵（即ち、”極秘”と分類された安全化されたファイルに主に指定された最も高いセキュリティレベル）は、全ての安全化された秘密に扱われるファイル２４８をアクセスするために使用でき、一方レベル２の使用許可鍵は、”極秘”と分類された安全化されたファイル以外の、全ての安全化された秘密に扱われるファイル２４８をアクセスするために使用できる。同様に、レベルＮの使用許可鍵は、セキュリティレベルＮの安全化されたファイルをアクセスするためにのみ使用できる。そのような配置の優位点の１つは、ユーザが、それらの安全化された秘密に扱われるファイルをアクセスする必要がある場合に、ユーザは、１つの使用許可鍵のみを有すればよいことである。

【００３７】図２Ｄは、本発明の他の実施例に従った、使用許可鍵を発生する図を示す。鍵発生器２４４は、主鍵２４６と補助鍵２４７として英数字又は２値数のいくつかの組みを発生するために、図２Ｂの２２６で決定されるセキュリティレベルを制御する、１つ又はそれ以上のパラメータ２４２を受信する。主鍵２４６は、決定されたセキュリティレベルにしたがって発生された、要求されたものであり、そして、セキュリティ又は秘密レベルで分類された安全化されたファイルにアクセスすることを容易にするのに使用され得る。補助鍵２４７は、そのセキュリティ又は秘密レベルよりも低く分類された安全化されたファイルにアクセスすることを容易にするのに発生される鍵である。図に示されたように、主鍵２４６はレベル２に分類された安全化されたファイルをアクセスするためのものであると仮定される。従って、補助鍵２４７はそれぞれ、セキュリティ又は秘密性に関してレベル２よりも低いすべての、レベル３、レベル４、．．．レベルＮに分類された安全化されたファイルをアクセスするのに使用される。本発明の説明を容易にするために、以下の説明は図２Ｃに基づいており、そして、図２Ｄに容易に適用できる。

【００３８】図２Ｂに戻ると、２２８で適切な使用許可鍵は発生された後に、使用許可鍵は２３０で、アカウントと関連させられ、それにより、ユーザは、使用許可鍵を必要とする安全化されたファイルをアクセスするのに正しい鍵を使用する。処理２２０は、２３２で、使用許可鍵についての読み出しを待つ。実行に依存して、使用許可鍵は、ローカルに又は遠隔的に格納されそして、安全化された秘密に扱われるファイルへアクセスする必要のあるときのみ取り出し可能である。ある場合には、使用許可鍵は、ユーザが第２の認証手段を通過するときのみ取り出し可能である。例えば、ユーザが少なくともあるセキュリティレベルで、秘密に扱われるある安全化されたファイルをアクセスする資格がある。ユーザに関連する使用許可鍵は、使用許可鍵のセキュリティレベルを増加させるために、生物測定学的情報確認又は第２のパスワードのような、第２の認証により、保護されるように構成される。非安全化された秘密に扱われるファイルがアクセスされるときに、使用許可鍵は必要ではなく、且つ従って、ユーザについて開放されず又は活性化されない。安全化された秘密に扱われるファイルがアクセスされるときには、処理２２０は２３４に進み、ここで、使用許可鍵は、必要なら、ユーザが必要な情報を完了したか又は、２次認証を通過した場合に、安全化されたファイル内のファイル鍵の取り出しを容易にするために、ユーザに開放される。

【００３９】図３Ａは、ヘッダ３０２と暗号化されたデータ部分３０４を有する、安全化されたファイル３００の例示の構造を示す。実行に依存して、ヘッダ３０２は、フラグ又は署名３０６を、含んでも含まなくてもよい。ある場合には、フラグ又は署名３０６は、他のファイルの中の安全化されたファイルのセキュリティの性質の検出を容易にするために使用される。ヘッダ３０２は、ファイル鍵ブロック３０８、鍵ブロック３１０及び規則ブロック３１２を含む。ファイル鍵ブロック３０８は、保護鍵３２０（即ち、しばしばｄｏｃ－ｋｅｙ鍵）と、更に安全化されたファイル３００にアクセスしようとするユーザに関連する使用許可鍵３２２での暗号器により暗号化されたファイル鍵３０９を含む。代わりに、ファイル鍵３０９は、使用許可鍵３２２としして保護鍵３２０により暗号化される。保護鍵３２０は、暗号化されそして、鍵ブロック３１０に格納される。一般的には、鍵ブロック３１０は保護鍵３２０の暗号化版を有

し、そして、指定されたユーザ又はグループによってのみアクセス可能である。ヘッダ内には１つ以上の鍵ブロックがあり、ここでは、図３Ａに３つの鍵ブロックが示されている。保護鍵３２０の保護を回復又は取り出すために、指定されたユーザは、規則ブロック３１２内の埋めこまれたアクセス規則でのアクセス規則テストを通過するために、適切なアクセス権を有しなければならない。

【００４０】全てのアクセス規則は、ユーザ鍵（例えば、公開ユーザ鍵）で暗号化され、そして、規則ブロック３１２内に格納される。安全化されたファイルにアクセスしようとするユーザは、規則ブロック３１２内のアクセス規則を復号するために、適切なユーザ鍵（例えば、秘密ユーザ鍵）を有しなければならない。このアクセス規則は、ユーザのアクセス権を測定するために適用される。ユーザがアクセス規則に関して安全化されたファイルにアクセスすることを許されている場合には、鍵ブロック３１０内の保護鍵３２０は、暗号化されたデータ部分３０４にアクセスするために、ファイル鍵３０９を取り出すために取り出される。しかしながら、安全化されたファイルが秘密であると検出された場合には、これは、保護鍵のみではファイル鍵を取り出せないことを意味し、ユーザは使用許可鍵を所有せねばならない。ユーザが、保護鍵３２０とともに使用許可鍵を有するときのみ、ファイル鍵３０９は、暗号化されたデータ部分３０４の復号を進めるために取り出されることができる。

【００４１】一実施例に従って、暗号化されたデータ部分３０４は、非安全化されたファイルを復号することにより生成される。例えば、非安全化された文書は、オーサリングツール（例えば、マイクロソフトワード（登録商標））で生成できる。非安全化された文書は、ファイル鍵で暗号化される。暗号化情報とファイル鍵は、そして、セキュリティ情報内に蓄積される。

【００４２】他の実施例に従って、非安全化された文書（データ）は、ＣＢＣモードを使用する強い暗号、暗号化されたデータへの高速なランダムアクセス、そして、完全性検査、の特徴を使用して暗号化される。このために、データはブロックで暗号化される。各ブロックのサイズは、予め定められた数又は、文書に特定である。例えば、予め定められた数は、暗号化機構で使用される実際の暗号ブロックサイズの倍数でもよい。一例は、ブロック暗号（即ち、固定長ブロックのプレーンテキスト（未暗号化テキスト）データを同じ長さの暗号化テキスト（暗号化テキスト）ブロックに変換する対称鍵暗号アルゴリズム）である。この変換は、暗号鍵（即ち、ファイル鍵）の動作の元で発生する。復号は、暗号化に使用されたのと他の暗号鍵又は同じ暗号鍵を使用して、暗号テキストブロックに逆変換を適用することにより行われる。固定長は、ブロックサイズと呼ばれ、６４ビット又は、１２８である。各ブロックはＣＢＣモードを使用して暗号化される。唯一の開始ベクトル（ＩＶ）は、各ブロックについて発生される。

【００４３】非安全化されたデータの他の暗号化は、ここの記載に関して、設計されることが可能である。どのような場合にも、暗号化情報とファイル鍵は、セキュリティ情報内に格納される。本発明の重要な特徴の１つは、ヘッダと暗号化されたデータ部分の統合は、安全化されていないデータの元々の意味を変えないことである。言い替えると、指定されたアプリケーションは、安全化されたファイルが選択され又は、”クリックされた”ときに、まだ活性化される。例えば、文書”ｘｙｚ．ｄｏｃ”は、選択されたときに、クライアントマシンで普通に見られるように、オーサリングツール、マイクロソフトワード（登録商標）を活性化する。文書”ｘｙｚ．ｄｏｃ”が本発明に従って安全化された後に、安全化されたファイルはユーザが認証され、ユーザは適切なアクセス権と十分なセキュリティ使用許可を有することを確認する処理通していかねばならないことを除いては、結果の安全化されたファイルは、まだ同じオーサリングツールを活性化できる、同じ”ｘｙｚ．ｄｏｃ”に見えるようになされる。

【００４４】本発明の重要な特徴の他の１つは、保護鍵の使用である。保護鍵で、ファイル鍵は、鍵ブロックを修正しなければならないこと無しに更新できる。例えば、ファイル鍵ブロック３０８内のファイル鍵は、鍵ブロックを修正しなければならないこと無しに更新できる。この特徴は、安全化されたファイルのセキュリティを改善するのを助け、そして、ファイルコピー操作をより高速に動作するようにする。

【００４５】図３Ｂは、本発明の一実施例に従った、安全化されたファイルの例示のヘッダ構造３５０を示す。一般的には、安全化されたファイルのヘッダは、安全化されたファイルのエントリの点である。ヘッダ構造３５０は、十分なアクセス権を有する認可されたユーザのみが、安全化されたファイル内の暗号化されたデータにアクセスできることを保証する種々のセキュリティ情報を含む。セキュリティ情報は、暗号的に保護され且つ安全にされている。一実施例では、ヘッダ又はセキュリティ情報の良好な部分は、有効な復号鍵又は、図３ＡのＣＲＣ３１６無しに、認可されていないユーザによりヘッダーと混ざったものを検出できる、メッセージ認証コード（ＭＡＣ）により保護されている。

【００４６】ヘッダ構造３５０は、好ましくは、マークアップ言語のような記述的言語に構造化される。そのようなマークアップ言語の例は、ＨＴＭＬ、ＷＭＬ、及びＳＧＭＬを含む。好ましい実施例では、マークアップ言語は、情報アクセスについてのポリシーを表すために本質的にＸＭＬ仕様である、拡張可能なアクセス制御マークアップ言語（ＸＡＣＭＬ）である。一般的には、ＸＡＣＭＬは、認可動作、アクセス要求者の特徴の効果、そ

れを介して要求がなされるプロトコル、活動のクラスに基づく認可及びコンテンツ内視（即ち、ターゲット内の要求者と属性値の両方に基づく認可で、ここで、属性値はポリシーライターに知られていない）の、きめの細かい制御と取り組める。更に加えて、ＸＡＣＭＬは、認可機構の実行を案内するために、ポリシー認可モデルを示すことができる。

【００４７】ヘッダ構造３５０内の１つの部分は、１つ又はそれ以上の鍵ブロックを含みうる鍵ブロックリスト３５２と呼ばれる。鍵ブロック３５４は、しばしば文書／ファイル暗号－鍵鍵と呼ばれる暗号化保護鍵、即ち、ファイル鍵への鍵である暗号化された保護鍵を含む。保護鍵が真に保護されていることを保証するために、それは暗号化され、そして、指定されたエンティティによってのみ取り出すことができる。例えば、安全化されたファイルが、エンジニアリンググループのメンバにより生成されそして、エンジニアリンググループの各メンバによより全アクセスが許される。同じ安全化されたファイルは、同時に、マーケティンググループの各メンバにより、制限されたアクセス（例えば、読み出しと印刷のみ）についても許される。従って、キーブロックリスト３５２は、１つはエンジニアリングの、そして、他はマーケティンググループのための、２つのキーブロックを含んでも良い。言い替えると、２つの鍵ブロックの各々は、（グループ又は個々の秘密鍵を介して）対応するグループのメンバによってのみアクセスされうる、暗号化保護鍵を有する。

【００４８】鍵ブロックバージョン値３５６は、保護鍵３４０を保護するのに使用される暗号化アルゴリズムの必要な詳細を提供する。一実施例では、ＲＳＡアルゴリズムとＯＡＥＰ法を組合せる公開鍵暗号機構である、ＲＳＡ－ＯＡＥＰ（ＲＳＡ－最適非対称暗号パディング（Ｏｐｔｉｍａｌ　Ａｓｙｍｍｅｔｒｉｃ　Ｅｎｃｒｉｐｔｉｏｎ　Ｐａｄｄｉｎｇ））が使用される。特に、鍵ペア３５８のｕｕｉｄは、証明書との値を復号するのに使用される、秘密鍵（詳細は示されていない）を識別する。加えて、鍵が１０２４又は２０４８ビット長であるかどうかのような、鍵ペアの属性は、保護鍵３４０の保護の保護を容易にするために含まれる。

【００４９】ヘッダ構造３５０のブロック３４２は、少なくとも３つのセグメント３４４、３４６及び３４８を有する。セグメント３４４は、暗号化されたデータ部分を復号するために明確に取り出されねばならない、暗号化されたファイル鍵を含む。セグメント３４６は、安全化されたファイルが例えば、”極秘”、”機密”、“秘密”、又は、”非秘密”又は、”無し”のどのセキュリティレベルかを示す、セキュリティレベル情報を含む。セグメント３４８は、安全化されたファイル内の暗号化されたデータ部分についての暗号ブロックのサイズに関する情報を含む。一実施例に従って、これは、アルゴリズムの暗号化ブロックサイズの倍数である。暗号化されたデータ部分は、文書／ファイル暗号鍵又はファイル鍵とここでは呼ばれる、対称鍵の暗号により生成される。

【００５０】ユーザ又は、グループ鍵により暗号化されたヘッダ構造３５０の他の部分３６０がある。部分３６０（詳細は示されていない）は、安全化されたファイルをアクセスするのはだれ／どこかを支配する安全化されたファイルに埋めこまれたアクセス規則を本質的に含む。ファイルをアクセスする種々の条件は、アクセス規則に置かれているか又は実現されている。アクセス規則の更なる詳細は、米国特許出願番号１０／０７４，８０４を参照する。

【００５１】上述の説明は、アクセス規則がユーザの公開鍵で暗号化された実施例に基づいている。当業者は、アクセス規則は、ファイル暗号化鍵（即ち、ファイル鍵）又は、保護鍵でも暗号化されてもよいことは、理解されよう。この場合には、保護鍵は、ユーザの公開鍵で又は、対称の安全化されたファイルが安全化される場合には、ユーザに関連する使用許可鍵と共に、暗号化される。安全化されたファイルにアクセスしようとするユーザのアクセス権に対してアクセス規則が成功的に測定された後に、保護鍵を取り出す代わりに、保護鍵は最初にユーザの秘密鍵と取り出される。保護鍵は、アクセス規則を取り出すのに使用され、保護鍵がアクセス規則を暗号化するのに使用された場合には、それは、続いて、ユーザのアクセス権に対して測定するのに使用される。ユーザが、ファイル内のコンテンツにアクセスすることが許される場合には、ファイル鍵はそして保護鍵と（又は、使用許可鍵と共に）取り出される。代わりに、保護鍵が取り出されたすぐ後に、保護鍵（又は、使用許可鍵と共に）は、ファイル鍵を取り出すのに使用される。ファイル鍵はそして、アクセス規則を取り出し、それは続いて、ユーザのアクセス権に対して測定するために使用される。いずれの場合にも、ユーザが、ユーザがアクセスポリシーに関して十分なアクセス権を有すると決定される場合には、もしあれば、取り出されたファイル鍵は、暗号化されたデータ部分の復号を継続するのに使用される。

【００５２】図４は、本発明の一実施例に従って、安全化されたファイルにアクセスする処理４００のフローチャートを示しそして、図３Ａと３Ｂと共に理解される。処理４００は、ユーザが安全化された文書にアクセスしようとするときに活性化される、実行可能なモジュール（例えば、文書安全化モジュール）で実行される。例えば、ユーザは、フォルダー、ローカルスは遠隔メモリ内に格納された安全化された文書にアクセスするために、マイクロソフト（登録商標）ウインドウズ（登録商標）オペレーティングシステムを実行するクライアントマシンを使用している。ウィンドウズエクスプローラ（登録商標）又は、インターネットエクスプローラ（登録商

標）を活性化することにより、ユーザはファイルのリストを表示し、幾つかは非安全化されそして、他は安全化されている。安全化されたファイルの中で、その幾つかは図３Ａに従った方法で、秘密にされ且つ安全化される。ファイルのリストの表示内で、望みの１つが選択される。代わりに、望みのファイルは、例えば、マイクロソフト（登録商標）アプリケーションのファイルの下に、”オープン”コマンドをを使用して、アプリケーションから選択される。

【００５３】いずれの場合にも、４０２で、そのような望みの文書は、アクセスされるべきと確認される。選択された文書を処理する前に、処理４００は、選択されたファイルが安全化されているか又は、非安全化を決定する必要がある。４０４で、選択された文書は、検査される。一般的には、選択された文書の安全性の特性を検査するのに少なくとも２つの方法がある。第１の可能な方法は、文書の先頭で、フラグ又は署名を探すことである。上述のように、ある安全化された文書では、予め定められたデータの組みのようなフラグは、安全化された文書のヘッダ内に置かれ、アクセスされている文書は安全化されていることを示す。フラグが見つからない場合には、処理４００は４２０に進み、即ち、選択された文書は、非安全化されているとみなされ、そして、従って、選択されたアプリケーションに又は、ユーザにより望まれる場所に送る又はロードすることを許す。第２の可能な方法は、選択された文書内でヘッダを捜すことである。安全化された文書であるならば、暗号化されたデータ部分に添付されたヘッダがある。ヘッダのデータフォーマットは、それが非安全化されている文書の場合の選択された文書と比較して、不規則である。選択されたアプリケーションにより要求されるように、選択された文書が不規則なデータフォーマットを有しない場合には、処理４００は４２０に進み、即ち、選択された文書は、非安全化されたとみなされ、そして、これは、選択されたアプリケーションに又はユーザにより望まれた場所に送られ且つロードされることを許す。

【００５４】４０４で、選択された文書が、真に安全化されていると決定する場合には、処理４００は４０６に進み、ここでは、ユーザ及び／又はユーザにより使用されているクライアントマシンは、ユーザ及び／又はクライアントマシンが認証されているかを決定するために検査される。ユーザが自分自身を認証することの詳細は、米国特許出願番号１０／０７４，８０４に記載されている。ユーザ及び／又はクライアントマシンが認証されていない場合には、処理４００は４１８に進み、これは、ユーザに適切なエラーメッセージを表示する。ユーザ及び／又はクライアントマシンが認証されていると仮定される場合には、そこのヘッダ又は、セキュリティ情報が、認証されたユーザ鍵で復号される。

【００５５】４０８で、復号されたセキュリティ情報内のアクセス規則が取り出される。上述のように、アクセス規則の組みがあり、各組みは、特定及びユーザ又は、特定のグループのメンバに指定されている。認証されたユーザ鍵及び／又は対応するユーザ識別子で、対応するアクセス規則の組みが取り出される。４１０で、取り出されたアクセス規則は、ユーザに関連する、アクセス権と比較（又は、それに対して測定）される。測定が失敗する場合には、これは、この特定の文書へアクセスすることがそのユーザには許されていないことを意味し、通知又は警告メッセージが、４１８で、ユーザに表示されるために、発生されうる。測定が成功的に通過した場合には、これは、この特定の文書へアクセスすることがそのユーザには許されていることを意味し、処理４００は、保護鍵を復号し且つ取り出すために４１１に進み、そして、安全化された文書が秘密扱いかどうかを、４１２で決定する。安全化された文書が秘密扱いでは無く、又は、セキュリティ情報内にセキュリティ使用許可情報要求がないと決定されるときには、処理４００は、４１６に進み、ここで、ファイル鍵が取り出され、そして、続いて、選択された（安全化された）文書内の暗号化されたデータ部分を復号するのに使用される。安全化された文書が秘密扱いであると決定されるときには、処理４００は、認証されたユーザはセキュリティ使用許可要求に合致する使用許可鍵を所有するかどうかを検査する４１４に進む。一般的には、使用許可鍵のセキュリティレベルは、安全化された秘密に扱われる文書内のセキュリティ使用許可要求と等しいか又は、それより高くなければならない。使用許可鍵のセキュリティレベルが十分でない場合には、処理４００は、ユーザに適切なエラーメッセージを表示するように構成された、４１８に進む。使用許可鍵のセキュリティレベルが十分である場合には、処理４００は、４１６に進む。

【００５６】いずれの場合にも、安全化された文書が秘密扱いでない場合には、ファイル鍵が保護鍵単独で、又は、安全化された文書が秘密扱いである場合には、使用許可鍵と共に保護鍵と取り出される。この結果、復号された文書又は、選択された文書のクリアなコンテンツが、４２０で供給される。

【００５７】図５は、本発明の一実施例に従って、生成されたファイル又は文書を安全化する処理５００のフローチャートを示す。処理５００は、マイクロソフトオペレーティングシステム（登録商標）を実行するクライアントマシンと共に理解される。しかしながら、当業者には、ここの説明又は、本発明は、そのような制限を意味しないことは、明らかである。

【００５８】５０２では、ブランクの文書が、選択されたオーサリングアプリケーションにより開かれ又は、生成され、そして、ユーザにより活性化される。オーサリングアプリケーションは、マイクロソフトワード（登録商標）、マイクロソフトパワーポイント（登録商標）又

は、ワードパーフェクト（登録商標）でもよい。好ましい手順では、ユーザは、文書を、アクセス規則と共に既に設定されている、フォルダー又は保護されたメモリに保存する。そうでない場合には、１つ又はそれ以上のアクセス規則が生成されてもよい。オプションで、アクセス規則は、望ましいアクセス規則、ユーザアクセス権のデフォルト又は、個々に生成されたユーザアクセス権を含む、前に生成されたファイルを持ち込むことにより受信されてもよい。５０４で、好ましくは、プレーンテキスト又は、マークアップ言語（例えば、ＸＡＣＭＬ）のような記述的言語で、予め定められたアクセス規則の組みが受信される。

【００５９】５０６で、秘密暗号鍵（即ち、ファイル鍵）が、文書についての暗号モジュールから発生され、そして、典型的には、通常のユーザにより一般的にはアクセスできない一時ファイルに内に典型的には、格納される。一時ファイルは、安全化されたファイルが成されたときに（例えば、アプリケーションからの”閉じる”コマンドで）、自動的に消去される。５０８で、ローカルメモリ内に文書を書き込む要求がなされたかどうかをみるために、文書はチェックされる。そのような要求が検出される場合には（ユーザにより手動で又は、オーサリングツール又は、ＯＳ手順により周期的に行われる）、文書は、５１０で、ファイル鍵により暗号化される。本発明の特徴の１つは、格納された文書は、なお処理されている場合でさえも（例えば、製作され、編集され又は、修正される）、常に、メモリ内に暗号化されることである。ユーザが文書を終わらせるときには、”閉じる”要求が活性化されて、文書を閉じる。５１２で、そのような要求が検出される。そのような要求が受信されるとすぐに、文書の安全化版はメモリに書きこまれる必要があることを意味する。５１４で、文書は秘密扱いされ、そして、文書を扱っているユーザは前に使用許可鍵が割り当てられたと仮定される。発生されたファイル鍵は、そして、保護／使用許可鍵で暗号化されそして、更に、使用許可／保護鍵で、暗号化される。保護鍵は、暗号化モジュールから発生されてもよい。５１６では、保護鍵が認証されたユーザ鍵により暗号化される。

【００６０】暗号化された保護鍵を保護するために、５１８で、適切なアクセス規則が適用されそして、暗号化された保護鍵と共に、認証されたユーザ鍵でさらに暗号化されうるセキュリティ情報に挿入される。セキュリティ情報の暗号化版は、そして、ヘッダに詰められる。実行に依存して、フラグ又は署名が更にヘッダに含められる。代わりに、ヘッダはフラグ無しのセキュリティ情報を含むことができる。５２０で、ヘッダは５１０からの暗号化された文書に添付され又は統合されそして、続いて、安全化された文書は５２４で、メモリに配置される。

【００６１】上述のように、安全化された文書は、暗号化されたセキュリティ情報を有するヘッダと、暗号化されたデータ部分（即ち、暗号化された文書）の、２つの暗号化された部分を有する。安全化された文書内の２つの部分は、２つの異なる鍵、ファイル鍵とユーザ鍵、でそれぞれ暗号化される。代わりに、２つの暗号化された部分は、５２２で、他の鍵で（又は、同じユーザ鍵を使用して）再び暗号化される。

【００６２】アクセス規則の幾つかの組みがある場合には、各々は特定のユーザについて又は、ユーザのグループについて、５１８で、暗号化されたアクセス規則は、図３Ａに示された規則ブロック内に、暗号化されたアクセス規則の他の組みと共に統合されることは、理解される。そのように、一人のユーザ又はグループからのアクセスは、他のユーザ又はグループに影響しないが、しかし、他のユーザ又はグループは、おそらく、暗号化された文書の更新版をみるであろう。

【００６３】図６は、本発明の例示の実行６００を示す。安全化されたファイルをアクセスするために又は生成されたファイルを安全化するために、ユーザにより使用されるクライアントマシンは、オペレーティングシステム（例えば、ＷＩＮＤＯＷＳ２０００／ＮＴ／ＸＰ（登録商標））を実行し、そして、１つ又はそれ以上のユーザモードのそして、他は、ＯＳモードの、２つの動作モードを有すると見られる。本発明の実行可能な版を表すクライアントモジュール６０２は、文書が安全化され且つ安全化された文書が、認可されたユーザによってのみアクセスできるようにされることを保証するために、オペレーティングシステム６０４と対話し且つオペレーティングシステム内で動作するように構成される。クライアントモジュール６０４の特徴は、その動作は、ユーザに透明であることである。いかえると、ユーザは、安全化された文書をアクセスする又は文書を安全化するときには、クライアントモジュール６０４の動作を知るようにはなされない。

【００６４】アプリケーション６０６（例えば、マイクロソフトワード（登録商標）のような登録されたアプリケーション）は、ユーザモードで又はＯＳ６０４モードで動作し、そして、メモリ６０８内に蓄積された文書にアクセスするために、活性化されうる。メモリ６０８は、ローカルストレージ場所（例えば、ハードディスク）又は、遠隔的に配置されている（例えば、他の装置）。アクセスされている文書の安全性の特徴（安全化対非安全化）に依存して、クライアントモジュール６０２は、鍵メモリ６０９（又は、それへのインターフェース）と暗号化モジュール６１０を活性化しても良い。鍵メモリ６０９は、ユーザが認証された後に認証されたユーザ鍵を維持する。ユーザが、ある安全化された秘密に扱われるファイルをアクセスする必要を有する場合には、鍵メモリ６０９は、対応する使用許可鍵を維持する。実行に依存して、鍵メモリ６０９は、他の位置から

使用許可鍵を取り出す又は、その暗号化版から使用許可鍵を活性化するように構成されてもよい。暗号化モジュール６１０は、１つはそれ以上の暗号化／復号機構を実行し、そして、代わりの暗号化／復号機構を実行する異なる暗号モジュールが、望まれるならば、容易く使用されるように、モジュール方式が好ましい。

【００６５】一実施例に従って、クライアントモジュール２０２は、本質的には、オペレーティングシステムの更に一般的な入力／出力命令を、サポートされているデバイス／モジュールが理解できるような、メッセージに変換する、デバイスドライバと多くの点で似ている。本発明のが実行されるＯＳに依存して、クライアントモジュール６０２は、ＶｘＤ（仮想デバイスドライバ）、カーネル又は、他の適用可能なフォーマットとして実行されてもよい。

【００６６】動作では、ユーザは、アプリケーション６０６（例えば、ＭＳＷＯＲＤ（登録商標）、パワーポイント（登録商標）又は、印刷）に関連する、文書を選択する。アプリケーション６０６は、文書に関して動作し、そして、インストール可能なシステム（ＩＦＳ）マネージャ６１２にアクセスするために、ＡＰＩ（例えば、ｃｒｅａｔｅＦｉｌｅ、ＭＳ　Ｗｉｎｄｏｗｓ（登録商標）内のＷｉｎ３２ＡＰＩを有する共通のダイアログファイルオープンダイアログ）を呼出す。”開く”要求がアプリケーション２０６からなされたことが検出される場合には、要求された文書にアクセスするために、要求は、適切なファイルシステムドライバ（ＦＳＤ）６１４に送られる。要求された文書が安全化されていることが検出されるときには、鍵メモリ２０９と暗号化モジュール６１０は、活性化されそして、認証されたユーザ（秘密）鍵が取り出される。要求された安全化された文書内のヘッダ内の暗号化されたセキュリティ情報は、ユーザ鍵で復号される。現在安全化された文書内のアクセス規則が有効なので、規則測定が、ユーザが選択された安全化された文書にアクセスすることを許されているかどうかを決定するために、クライアントモジュール６０２内で実行される。測定が成功である場合には、これは、ユーザが安全化された文書をアクセスすることを許されていることを意味し、ファイル鍵が、使用許可鍵だけでなく取り出された保護鍵で、セキュリティ情報から取り出され、そして、続いて、暗号化モジュール６１０が、クライアントモジュール６０２内の、安全化された文書（即ち、安全化されたデータ部分）を復号することを進行する。クリアなコンテンツが、そして、ＩＦＳマネージャ６１２を通してアプリケーション６０６に戻される。例えば、アプリケーション６０６がオーサリングツールである場合には、クリアなコンテンツが表示される。アプリケーション６０６が印刷ツールである場合には、クリアなコンテンツは指定されてプリンタに送られる。

【００６７】他の実施例では、ＰｒｏｃｅｓｓＩＤプロパティとして知られている、オペレーティングシステム（ＯＳ）アクセスは、（ＡｐｐＡｃｔｉｖａｔｅメソッドの引数として）アプリケーションを活性化するのに使用される。ＰｒｏｃｅｓｓＩＤは、アプリケーションを識別し、そして、そのイベントハンドラは、異なるファイルシステム構成要素へのアクセスを仲裁する責任のある、インストール可能なファイルシステム（ＩＦＳ）マネージャ６１２へのＯＳアクセスを継続するために必要なパラメータを取る。特に、ＩＦＳマネージャ６１２は、ファイルのオープン、クローズ、読み出し、書きこみ等のような種々の動作を実行するエントリー点として動作する。従って詰められた１つ又はそれ以上のフラグ又はパラメータで、アクセスは、クライアントモジュール６０２を活性化する。アプリケーションによりアクセスされている１つの文書が通常の（非安全化の）場合には、文書は、ファイルシステムドライバ（ＦＳＤ）（例えば、ＦＳＤ６１４）からフェッチされそして、クライアントモジュール６０２に送られ、そして続いて、ＩＦＳマネージャ６１２を通してアプリケーションにロードされる。一方では、アプリケーションによりアクセスされている文書が安全化されている場合には、クライアントモジュール６０２は、鍵メモリ６０９と暗号化モジュール６１０を活性化し、そして、そこのアクセス規則を取り出すために、認証されたユーザ鍵を得ることを進める。鍵メモリ６０９からのアクセステストからの結果を未決定とし、ファイル鍵は、暗号化モジュール６１０内の暗号器により安全化された文書の暗号化されたデータ部分を復号するために、取り出されうる。この結果、クリアモードのデータ部分又は文書が、ＩＦＳマネージャ６１２をとしてアプリケーションにロードされる。

【００６８】本発明を、ある程度の特殊性で、十分詳細に説明した。当業者には、実施例の本開示は、例示目的のみであり、配置と部品の組合せの多くの変更は、請求の範囲に記載の本発明の意図と範囲から離れること無しに、行われうることは理解されよう。従って、本発明の範囲は、実施例の前述の説明よりも、添付の請求の範囲により画定される。

【００６９】

【発明の効果】上述のように、本発明により、常に、ディジタル資産を安全にし且つ保護する更に効果的な方法を提供できる。

【図面の簡単な説明】

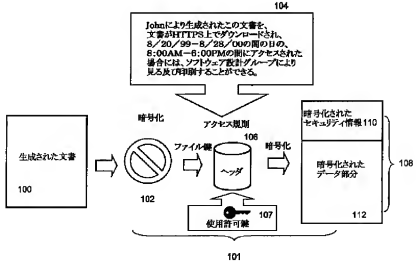
【図１】本発明で使用される一例の安全化されたファイル形式に従って、生成された文書を安全化する図を示す。

【図２Ａ】本発明の一実施例に従って、２つの貫かれたアクセス機構と呼ばれるものを示す図である。

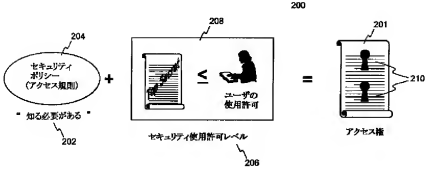
【図２Ｂ】本発明の一実施例に従った、適切なセキュリティ使用許可レベル（即ち、使用許可鍵）を許可する処

理のフローチャートを示す図である。
【図２Ｃ】本発明の一実施例に従った、使用許可鍵の発生を示す図である。
【図２Ｄ】本発明の他の実施例に従って、使用許可鍵を発生する図を示す。
【図３Ａ】ヘッダと暗号化されたデータ部分を含む安全化されたファイルの例示の構造を示す図である。
【図３Ｂ】本発明の一実施例に従った安全化されたファイルの例示のヘッダ構造を示す図である。
【図４】図３Ａと図３Ｂと共に理解され且つ本発明の一実施例に従って安全化された文書をアクセスする処理のフローチャートを示す図である。
【図５】本発明の一実施例に従って生成されるファイル又は文書を安全化する処理のフローチャートを示す図である。
【図６】本発明の例示的な実行を示す図である。
【符号の説明】
１００　文書
１０１　安全化処理
１０２　暗号化処理
１０４　アクセス規則
１０６　ヘッダ
１０７　セキュリティ使用許可情報
１０８　安全化されたファイル
１１０　暗号化されたセキュリティ情報
１１２　暗号化されたデータ部分
２０１　安全化されたファイル
２０４　アクセス規則
２０６　セキュリティ使用許可レベル
２４４　鍵発生器
２４６　鍵
２４６　主鍵
２４７　補助鍵
３００　安全化されたファイル
３０２　ヘッダ
３０４　暗号化されたデータ部分
３０６　フラグ又は署名
３０６　署名
３０８　ファイル鍵ブロック
３０９　ファイル鍵
３１０　鍵ブロック
３１２　規則ブロック
３２０　保護鍵
３２２　使用許可鍵
３４０　保護鍵
３４４、３４６及び３４８　セグメント
３５０　ヘッダ構造
３５２　鍵ブロックリスト
３５４　鍵ブロック
３５６　鍵ブロックバージョン値
３５８　鍵ペア
６０２　クライアントモジュール
６０６　アプリケーション
６０８　メモリ
６０９　鍵メモリ
６１０　暗号化モジュール
６１２　ＩＦＳマネージャ
６１４　ファイルシステムドライバ（ＦＳＤ）

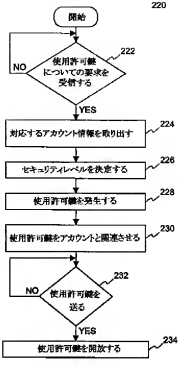
【図１】



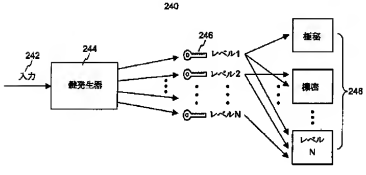
【図２Ａ】



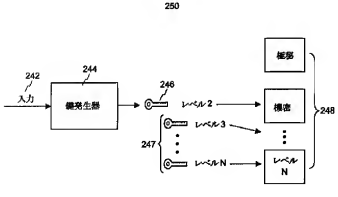
【図２Ｂ】



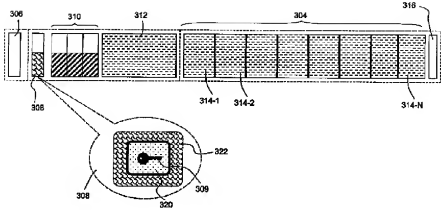
【図２Ｃ】



【図２Ｄ】



【図３Ａ】



【図３Ｂ】

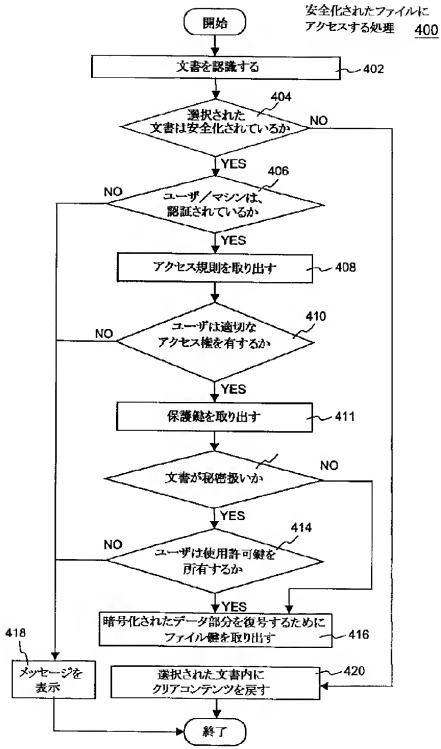
350

Header (Version 1)

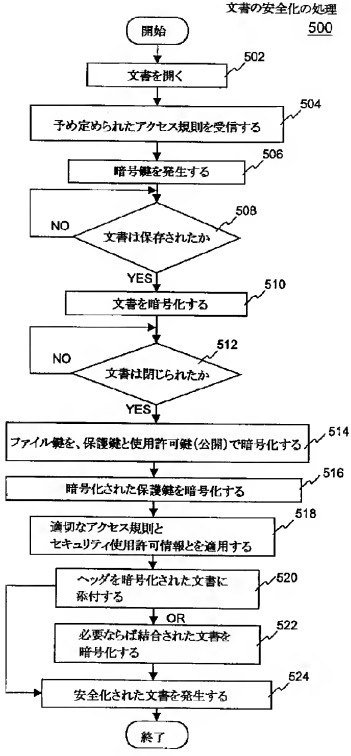
```
<header version="1.0" document_uuid="...">
  <key_block_list version="1.0">
  <key_block version="1.0" group_uuid="..."> 356
  </key_block>
    <key_block version="1.0" group_uuid="..">
    <document_encryption_key_key key_pair_uuid="..."> 354
      ... (Encrypted protection key) 358
    </document_encryption_key_key>
  </key_block> 340
      ... (more blocks if necessary)
  </key_block_list>

  <document_crypto_info version="...">
      <document_crypto version="1.0">
    <enc_doc_key>... (Encrypted document-encryption-key) 344
    </enc_doc_key>
    <enc_doc_level> ... (String like "Secret" or "Top Secret" or "None") 346
    </enc_doc_level>
    <encryption_algorithm name="..." key_size="..." block_size="..." /> 348
    <sea_block_size>... (size of encryption size)
    </sea_block_size>
      </document_crypto>
  </document_crypto_info>

  <enc_document_information>
      <document_information version="1.0">
        <creation creator_uuid="..." date="..." / >
        <last_modification modifier_uuid="..." date="..." / >
    <rule_set>... (details omitted) 360
    </rule_set>
      <document_information>
  </enc_document_information>
</header>
<header_MAC version="..."> ... (See Header MAC Information)
</header_MAC>
```

352 342

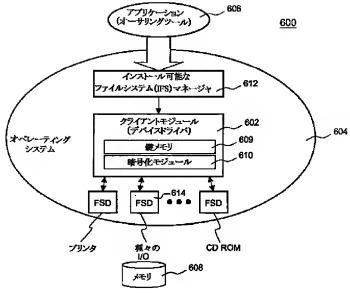
【図４】


安全化されたファイルに
アクセスする処理 400
開始
文書を認識する
402
選択された
文書は安全化されているか
404
NO
YES
ユーザ／マシンは、
認証されているか
406
NO
YES
アクセス規則を取り出す
408
ユーザは適切な
アクセス権を有するか
410
NO
YES
保護鍵を取り出す
411
文書が秘密扱いか
NO
YES
ユーザは使用許可鍵を
所有するか
414
NO
YES
暗号化されたデータ部分を復号するために
ファイル鍵を取り出す
416
418
メッセージを
表示
選択された文書内に
クリアコンテンツを戻す
420
終了

【図５】


文書の安全化の処理
500
開始
502
文書を開く
504
予め定められたアクセス規則を受信する
506
暗号鍵を発生する
508
NO
文書は保存されたか
YES
510
文書を暗号化する
512
NO
文書は閉じられたか
YES
514
ファイル鍵を、保護鍵と使用許可鍵(公開)で暗号化する
516
暗号化された保護鍵を暗号化する
518
適切なアクセス規則と
セキュリティ使用許可情報とを適用する
520
ヘッダを暗号化された文書に
添付する
OR
522
必要ならば結合された文書を
暗号化する
524
安全化された文書を発生する
終了

【図６】



フロントページの続き

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０９Ｃ 1/00	６６０	Ｈ０４Ｌ 9/00	６０１Ａ

(72)発明者 デニス ジャック ポール ガルシア
アメリカ合衆国 カリフォルニア州 94304 パロ・アルト オーク・クリーク・ドライヴ 1736 アパートメント・204号

Ｆターム(参考) 5B017 AA03 BA06 BA07 CA16
5B082 EA11 GA11
5J104 AA12 AA16 EA04 EA08 EA15 NA02 PA14